Revista Pleiade – Centro Universitário Descomplica UniAmérica
ISSN 1980-8666 (Impresso) – ISSN 2674-8231 (Eletrônico) – Classificação Capes B3 (2017-2020)

Preservação de Privacidade em Dispositivos IoT Conectados a Redes Blockchain: Revisão Sistemática de Literatura

Privacy Preservation in IoT Devices Connected to Blockchain Networks: Systematic Literature Review

Fabio Augusto Frasson[1], Willian Vieira Costa Zonatto[2], Ruminiki Pavei Schmoeller[3] e Isabel Fernandes[4]

1. Acadêmico concluinte de Bacharelado em Engenharia de Software do Centro Universitário UniAmérica. 2. Bacharel em Direito e Ciências Contábeis. Mestre em Sociedade, Cultura e Fronteiras. Especialização em Segurança Pública; Gestão de Organizações Públicas; Gestão do Sistema Prisional. Titular do Conselho Penitenciário do Paraná (COPEN). Suplente do Conselho Diretor do Fundo Penitenciário do Paraná (CED/FUPEN). Docente Ensino Superior e Escola de Formação e Aperfeiçoamento Penitenciário do Paraná (ESPEN). 3. Informática. Especialista em Data Science e Analytics. Mestrado em Tecnologias Computacionais para o Agronegócio. Professor Bacharelado em Engenharia de Software. https://orcid.org/0009-0006-5046-4390 4. Computação. Doutora em Engenharia da Produção. Professora do Centro Universitário Descomplica UniAmérica. https://orcid.org/0000-0002-6906-5756
fabio.frass@gmail.com e isabel.souza@descomplica.com.br

Palavras-chave
Blockchain
Internet of Things
Privacidade

Keywords
Blockchain
Internet of Things
Privacy

Resumo:
Introdução. Com o avanço das tecnologias da informação e comunicação (TIC), se faz presente uma preocupação cada vez mais latente com a privacidade do usuário e a aplicação de normativas governamentais. Objetivo. Apresentar os resultados de uma revisão sistemática da literatura (RSL) sobre a preservação da privacidade em dispositivos IoT presentes na rede Blockchain. Metodologia. A metodologia utilizada nesta RSL baseia-se no método proposto por Kitchenham e levou em conta as bases ACM Digital library, arXiv, IEEExplore e ScienceDirect. Ao todo, 821 trabalhos foram encontrados, e após aplicados os critérios de exclusão, 18 trabalhos foram selecionados para o escopo desta revisão. Resultados. Pouco mais da metade dos trabalhos analisados utilizam ao menos dois dos três domínios de pesquisa sugeridos, também foi possível elencar as tecnologias empregadas na operacionalização destes conceitos. Considerações Finais. É perceptível a preocupação com a privacidade do usuário em contextos IoT. Sugere-se a ampliação da classificação proposta para os demais domínios.

Abstract:
Introduction. With the advancement of information and communication technologies (ICT), there is an increasingly latent concern with user privacy and the application of government regulations. Objective. To present the results of a systematic literature review (SLR) on the preservation of privacy in IoT devices present in the Blockchain network. Methodology. The methodology used in this SLR is based on the method proposed by Kitchenham and took into account the ACM Digital library, arXiv, IEEExplore and ScienceDirect databases. In total, 821 works were found, and after applying the exclusion criteria, 18 works were selected for the scope of this review. Results. A little over half of the works analyzed use at least two of the three research domains suggested by Cha, and it was also possible to list the technologies used to operationalize these concepts. Final Considerations. The concern with user privacy in IoT contexts is noticeable. It is suggested to expand the proposed classification to the other domains.

Artigo recebido em: 16.10.2024.
Aprovado para publicação em: 14.11.2024.

INTRODUÇÃO

O recente salto no avanço da tecnologia possibilitou a criação de dispositivos inteligentes que vêm sendo amplamente incorporados ao nosso cotidiano, como relógios multifunções, aparelhos domésticos e carros inteligentes, entre outros. Utiliza-se o termo Internet of Things (IoT) para se referir a estes dispositivos que, conectados a uma tecnologia, podem se comunicar uns com os outros e também com a nuvem, além de possuir sensores e processadores incorporados. A propagação dessas tecnologias permitiu que esses dispositivos fossem inseridos até mesmo dentro de nossas casas (PAPPACHAN et al., 2017).

Entre alguns usos de IoT nesse contexto, podemos citar aquecimento, ventilação, iluminação, refrigeração e segurança. Área que recebe influência destes dispositivos é a chamada de smart buildings (edifícios inteligentes, em tradução livre), onde aparelhos tradicionais passaram a receber sinalizadores, sensores de presença, câmeras e dispositivos pessoais portados pelos habitantes desses edifícios. Entretanto, uma similitude nesses cenários é a dependência em coletar dados, o que contraria o que se espera no quesito privacidade (PAPPACHAN et al., 2017). Nesse sentido, muito vem se discutindo sobre questões ligadas a essa constante troca de dados, o seu tratamento, e ainda qual o controle dos usuários sobre suas próprias informações.

Com os avanços na inovação, na competição global e na complexidade dos sistemas, surgem novos desafios do ponto de vista da tecnologia da informação. A privacidade deve ser priorizada em sistemas de dados e tecnologias, se tornando assim parte nos processos prioritários, objetivos de projetos, design de processos e planejamento de operações, bem como ser incorporada em todos os momentos de nossa vida (CAVOUKIAN, 2009). Contudo, na prática, nem sempre os utilizadores estão cientes de quais informações estão sendo trocadas, nem com quais empresas, o que traz a importância do tema à tona.

Nesse sentido, confiar em sistemas de terceiros para o armazenamento de ativos pessoais se torna precário, já que podem ser hackeados, manipulados ou ainda comprometidos. Alternativa, sugerida por Crosby et al. (2016), é a utilização de tecnologia Blockchain, que tem o potencial de revolucionar o mundo digital ao permitir que cada transação, passada ou presente, possa ser verificada a qualquer momento no futuro. Isso é possível sem que haja comprometimento da privacidade dos ativos, uma vez que um dos pilares da tecnologia é o anonimato. Tendo essa premissa em mente, alguns trabalhos vêm sendo desenvolvidos e sugerem a utilização de mecanismos para aprimorar a preservação de privacidade dos usuários de dispositivos IoT.

Iniciativas pensadas de forma a possibilitar maior controle sobre os dados do usuário que são trafegados em aplicações, sua segurança, aderência a políticas governamentais sobre uso de dados, entre outros quesitos. Exemplo dessa natureza é o trabalho proposto por Cha et al. (2019), tecnologias de aprimoramento da privacidade (PETs) são definidas como extensivo conceito, que engloba todos os tipos de tecnologias, estruturas e aspectos de suporte à privacidade ou aos recursos de proteção de dados privados, além de aumentar o controle dos indivíduos sobre seus dados. Em sua obra, o autor sugere uma classificação de aplicações IoT por domínios de pesquisa, a fim de avaliar as várias proteções de privacidade que as PETs oferecem.

Considerando os domínios para avaliar as várias proteções de privacidade que as PETs, controle sobre os dados, implementação de diretrizes e anonimização ou pseudoanonimização, este estudo visa classificar aplicações IoT que utilizam tecnologia blockchain, com vistas a identificar as PETs presentes em sua arquitetura.

METODOLOGIA

Esta Revisão Sistemática da Literatura tomou por base a metodologia sugerida por Kitchenham et al. (2007), e foi desenvolvida considerando as seguintes etapas: elaboração das questões da pesquisa, definição

das bases para busca, definição da string de busca, critérios de inclusão e exclusão de trabalhos, e condução da busca. As subseções seguintes detalham melhor cada uma das etapas mencionadas.

1. Elaboração das Questões de Pesquisa

Com base no tema proposto, foi elaborada a questão norteadora do trabalho (QNT) e as questões auxiliares (QAs), que visam explorar trabalhos existentes e investigar mais a fundo os mecanismos de privacidade em aplicações IoT presentes na rede Blockchain. São elas:

QNT: Como é aplicada a preservação da privacidade em dispositivos IoT presentes na rede Blockchain?

QA1: Considerando os eixos propostos nas PETs, quais foram aplicados nos trabalhos?

QA2: Quais tecnologias possibilitaram a implementação desses eixos?

2. Definição das Bases para Busca

Devido à sua importância para a área da Engenharia de Software (BRERETON et al., 2007) e agregando-se bases de preferência do pesquisador, quatro opções foram selecionadas:

1. ACM Digital library (https://dl.acm.org/);
2. arXiv (https://arxiv.org/);
3. IEEExplore (https://ieeexplore.ieee.org/Xplore/home.jsp);
4. ScienceDirect (https://www.sciencedirect.com/).

3. Definição da String de Busca

A string de busca foi elaborada a partir da estratégia População, Conceito e Contexto (PCC), descrita por Peters et al. (2015), que consiste nos elementos apresentados na Tabela 1. Os termos incluídos foram selecionados de forma a possibilitar a recuperação do maior número possível de trabalhos com vistas a responder à QNT e às QAs. Devido ao tema do trabalho ter sido pouco desenvolvido em trabalhos de língua portuguesa, a busca dos termos em língua inglesa possibilitou a recuperação de grande parte dos trabalhos utilizados nesta revisão. Optou-se por considerar também sinônimos dos termos, de forma a abarcar também as fontes primárias que porventura se dirijam ao tema utilizando as variações incluídas.

A string final de busca pode ser observada na Figura 1, onde foram aplicados os operadores OR (ou lógico) entre os sinônimos e AND (e lógico) entre os termos de pesquisa. Os termos apresentados são resultados de vários testes feitos nas bases mencionadas e ajustes, visto que o processo de definição da string de busca é iterativo e envolve vários ciclos de experimentação e verificação dos artigos retornados (DERMEVAL et al., 2020).

4. Critérios de Inclusão e Exclusão de Trabalhos

Foram selecionados estudos cujo título, resumo e palavras-chave estivessem de acordo com os termos da *string* de busca construída. Ademais, critérios específicos para inclusão e exclusão dos trabalhos foram aplicados, conforme mostrado na Tabela 2. A data de publicação considerada foi de no máximo 5 anos, de forma a analisar os trabalhos e conceitos mais atuais no que tange mecanismos de preservação de privacidade de usuários.

Tabela 1. Estratégia PCC

	P (População)	C (Conceito)	C (Contexto)
Extração	dispositivos IoT	preservação de privacidade	rede Blockchain
Sinônimos	IoT; internet of things	tecnologias de preservação de privacidade; tecnologias de aprimoramento da privacidade	blockchain; tecnologia de registro distribuído
Construção	(IoT OR internet of things)	(privacy-preserving solutions OR privacy-preserving technologies OR privacy-enhancing technologies)	(blockchain OR distributed ledger technology)

Fonte: Os autores.

Figura 1. *String* de busca

(*"IoT"* **OR** *"internet of things"*) **AND**
(*"privacy-preserving solutions"* **OR** *"privacy-preserving technologies"* **OR** *"privacy-enhancing technologies"*) **AND**
(*"blockchain"* **OR** *"distributed ledger technology"*)

5. Condução da Busca

A busca foi conduzida considerando-se as bases descritas na subseção 2.2 e utilizando-se a string de busca mencionada na subseção 2.3. Os critérios de inclusão e exclusão de trabalhos, contidos na subseção 2.4, foram aplicados com vistas a selecionar os trabalhos mais relacionados com o tema proposto.

Na busca geral, em primeira instância, foram retornados 821 trabalhos, dos quais 795 restaram após o filtro de período de publicação (Tabela 2, ID I-1). Um filtro para trabalhos primários também foi utilizado (Tabela 2, ID I-2), apesar de estar presente apenas nas bases ACM Digital Library e Science Direct. Respectivamente, nestes dois repositórios, foram reduzidos os números de trabalhos recuperados de 83 para 24, e de 223 para 140.

Ao se utilizar o critério I-3, que diz respeito à disponibilização dos trabalhos, restaram 0 trabalhos na ACM Digital Library, 4 na arXiv, 49 na IEEExplore e 41 na Science Direct. No quesito idioma e combinação de resumo e palavras-chave (I-4 e I-5), foram obtidos 3 trabalhos na base arXiv, 23 trabalhos na base IEEExplore e 8 trabalhos na base Science Direct. A figura 2 lista o fluxograma final do procedimento de recuperação das produções científicas.

Uma vez reduzido o número de trabalhos para 34, considerando-se os critérios de inclusão e exclusão, uma etapa de análise de qualidade foi iniciada para maior acurácia na apuração da extração de dados, o que ajuda também na credibilidade e síntese razoável dos resultados (DERMEVAL et al., 2020).

Tal etapa foi norteada por perguntas de qualidade (PQs), descritas a seguir: PQ1) O estudo visa, com o emprego da tecnologia, fortalecer a preservação da privacidade no contexto abordado? PQ2) A base do estudo leva em consideração os dispositivos IoT que utilizam tecnologia Blockchain? PQ3) Há explanação de como as características da Blockchain são empregadas para o objetivo de preservação da privacidade?

Cada pergunta de qualidade poderia ser respondida como 'Sim', 'Parcialmente' e 'Não', conferindo, respectivamente, 1 ponto, 0.5 ponto e 0 ponto. Somando-se a pontuação de todas as respostas, aqueles trabalhos

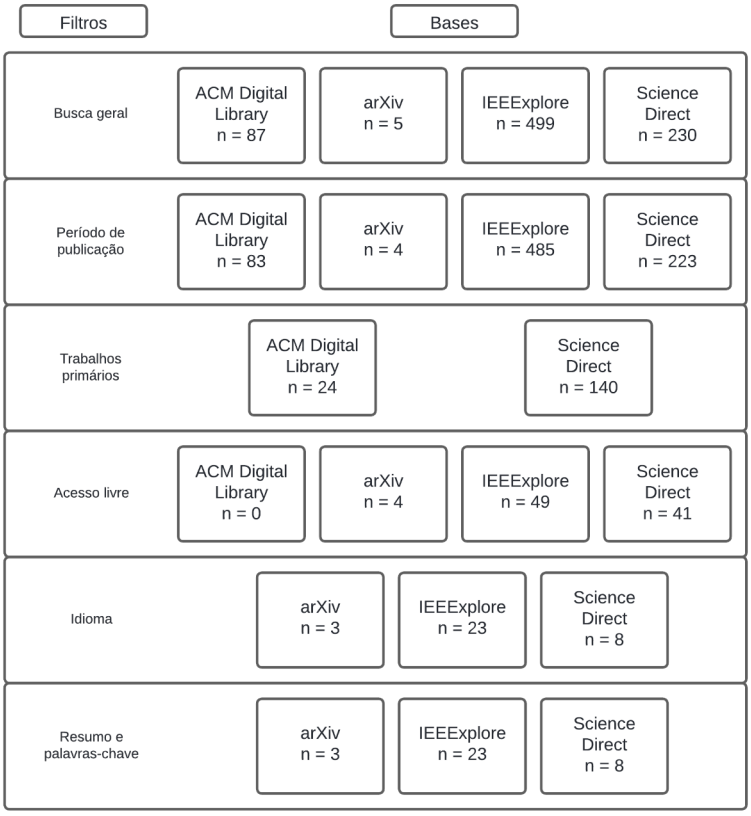
cuja soma fosse maior do que 2 pontos (66,6% do total possível de pontos) foram selecionados para utilização nesta revisão.

Tabela 2. Critérios de inclusão e exclusão de estudos

Tipo	ID	Descrição
Inclusão	I-1	Publicação há no máximo 5 anos
	I-2	Trabalhos primários (disponível apenas em algumas bases)
	I-3	Acesso livre
	I-4	Idioma seja português ou inglês
	I-5	Resumo e palavras-chave de acordo com o tema proposto
Exclusão	E-1	Data de publicação maior que 5 anos
	E-2	Trabalhos de revisão
	E-3	Acesso restrito
	E-4	Itens duplicados
	E-5	Trabalhos em idiomas não selecionados
	E-6	Estudos que fujam do tema sugerido

Fonte: Os autores.

Figura 2. Representação gráfica da condução da busca.



Fonte: Os autores.

Ademais, durante a etapa de triagem de qualidade, dois trabalhos foram identificados como trabalhos secundários, mesmo os critérios de inclusão e exclusão tendo sido aplicados. A base IEEExplore não dispunha de filtros para tipo de trabalho (primário, secundário, etc.) e a base Science Direct o dispunha, porém mesmo fazendo uso do recurso, um trabalho secundário permaneceu na lista.

Ao final, após concluída a análise de qualidade, foram elencados 18 trabalhos no total, os quais serão utilizados como base para esta revisão sistemática de literatura.

RESULTADOS

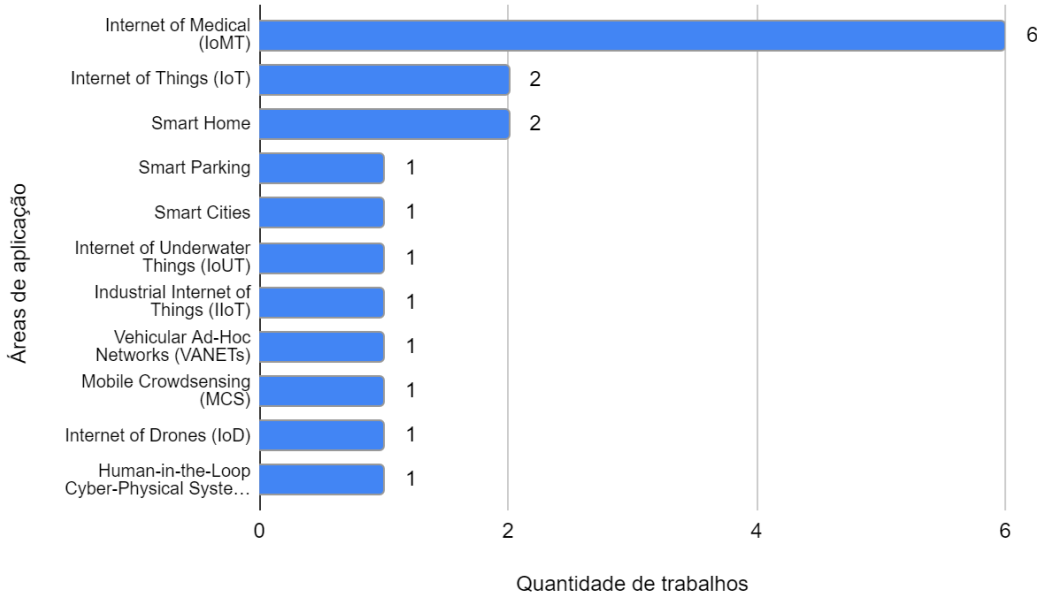
Esta seção apresenta os resultados obtidos a partir da extração de dados dos trabalhos selecionados, apoiada pelas questões auxiliares (QAs) apresentadas na seção 2.1. O primeiro passo foi extrair as variáveis caracterizadoras dos trabalhos selecionados, dispostas na seção 3.1, e as variáveis respondentes às questões da RSL e a discussão, apresentadas na seção 3.2.

1. CARACTERIZAÇÃO DOS ESTUDOS SELECIONADOS

Uma análise prévia foi realizada, com o intuito de extrair informações mais gerais sobre os trabalhos, tais como área de aplicação, país dos autores e ano de publicação dos estudos.

Inicialmente, a área de aplicação da tecnologia foi avaliada, a fim de traçar um panorama das áreas mais críticas, cujo foco fosse a preservação da privacidade do usuário. Parece ser evidente que a área médica (IoMT) lidera esse ranking, totalizando 6 estudos, seguida pelas áreas de Internet of Things (IoT - classificação atribuída aos trabalhos que não especificaram a área de aplicabilidade da proposta) e Smart Home. Os demais estudos mesclam áreas bem específicas, como Internet of Drones e Internet of Underwater Things (IoUT). Mais detalhes podem ser visualizados na Figura 3.

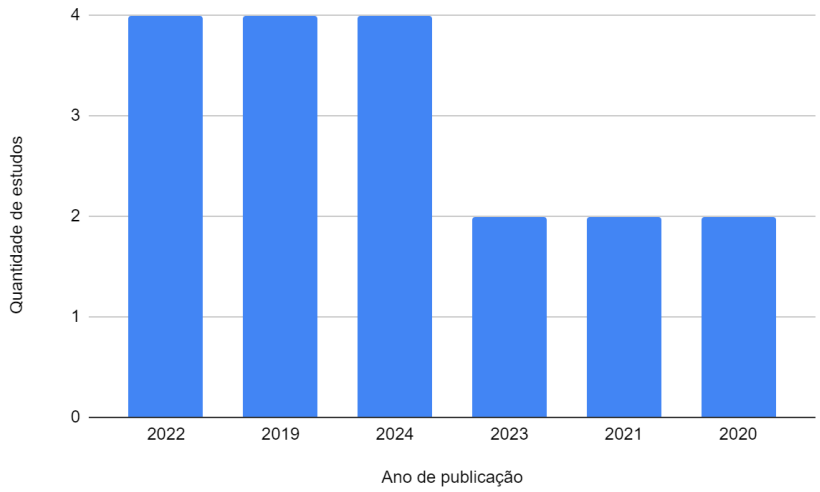
Figura 3. Áreas de aplicação x quantidade de trabalhos.



Fonte: Os autores.

O segundo aspecto analisado foi o ano de publicação dos trabalhos (Figura 4), cujas maiores frequências encontram-se em 2019, 2022 e 2024, com 4 itens cada. Entretanto, apesar do corte temporal feito durante a busca (critério I-1), notou-se que a maioria dos trabalhos envolvendo Blockchain e dispositivos IoT com enfoque na preservação da privacidade são bem recentes.

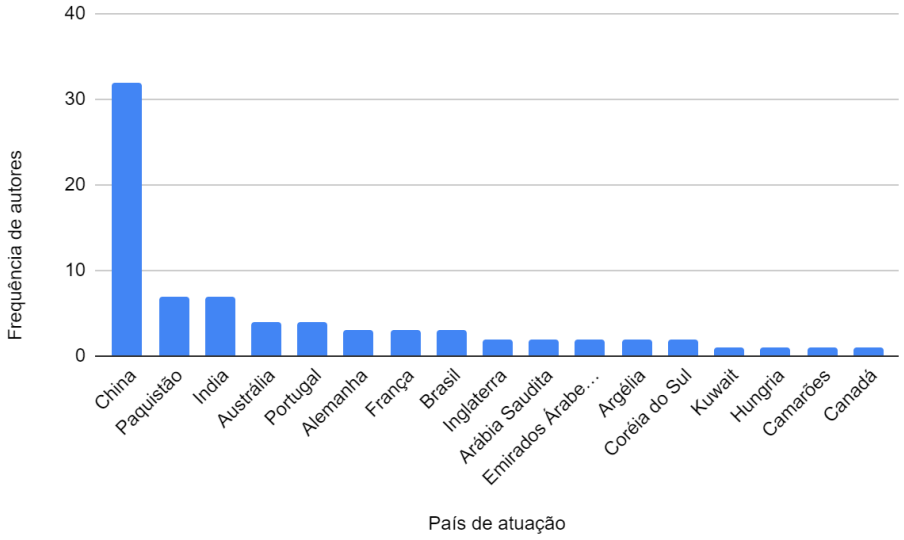
Figura 4. Áreas de aplicação x quantidade de trabalhos



Fonte: Os autores.

Outro aspecto importante para a descoberta do panorama atual do estado da arte é o país de atuação dos autores, indicativo de quais países produzem mais pesquisas na área. Considerando os trabalhos selecionados, é observado o protagonismo da China, seguida pelo Paquistão e pela Índia, respectivamente em segundo e terceiro lugares. Todos os países de atuação dos autores e frequências podem ser visualizados na Figura 5.

Figura 5. Áreas de aplicação x quantidade de trabalhos



Fonte: Os autores.

2. Classificação das Tecnologias e Discussão

Os 18 artigos revisados apresentam abordagens distintas, que foram aplicadas em áreas específicas de IoT, visando a preservação da privacidade dos dados trafegados. De acordo com o trabalho de Cha et al. (2019), considerando os eixos i. controle sobre os dados, ii. implementação de diretrizes e iii. anonimização ou pseudoanonimização, os estudos mencionados foram classificados de acordo com as tecnologias presentes em cada uma de suas arquiteturas (Tabela 3).

O primeiro grupo, controle sobre os dados, refere-se à característica de fornecer maior controle sobre os dados pessoais dos usuários, incluindo quais informações podem ser coletadas, a forma de processamento e local de armazenamento, assim como quem está permitido a acessá-las e ainda para qual finalidade. Essa medida previne que empresas terceiras, de posse desses dados, possam abusar dessas informações sensíveis sem consentimento do usuário (CHA et al., 2019).

Já o segundo grupo, conforme Cha et al. (2019), denominado implementação de diretrizes, diz respeito à execução de políticas de privacidade e restrições no acesso aos dados sensíveis. Esse conjunto de regras permite que usuários especifiquem seus dados pessoais sejam tratados por provedores de serviços, enquanto limitam acesso não autorizado. Através de suas configurações, apenas aqueles dados sensíveis habilitados pelo usuário poderão ser enviados para empresas terceiras, agindo como barreira de proteção.

No terceiro grupo, temos a anonimização ou pseudoanonimização, que apesar de semelhantes, são duas técnicas distintas. A anonimização consiste na eliminação não reversível dos dados identificáveis (sensíveis), de forma a evitar que o indivíduo seja reconhecido, enquanto a pseudoanonimização é um método reversível, desde que as chaves utilizadas no processo estejam disponíveis (CHA et al., 2019). Com base nas definições apresentadas nos parágrafos anteriores, os trabalhos desta revisão foram mapeados conforme os eixos propostos por Cha et al. (2019), levando em consideração as tecnologias presentes em cada proposta. Supõe-se que apenas um dos trabalhos tenha incorporado os três eixos sugeridos pelo autor (SAIDI et al., 2022), e que 9 tenham apresentado simultaneamente dois eixos. O mapeamento completo é visualizado na Tabela 3.

Para aclaração dos eixos identificados na Tabela 3, a começar por i. controle sobre os dados, percebe-se que diferentes tipos de sistemas de controle de acesso foram empregados nos estudos analisados. Como exemplos, é possível citar sistema de controle de acesso a dados baseado em blockchain, com foco na privacidade BPADAC (MA, Z.; ZHANG, J., 2023), sistema de controle de acesso a dados descentralizado e autogerido, ou DSMAC (SAIDI et al., 2022) e sistema de controle de acesso baseado em cargos, RBAC (SUTRADHAR et al., 2024). Dos trabalhos revisados, apenas Zou et al. (2020) não continha mecanismos pertencentes à esfera avaliada.

Quanto ao eixo ii. implementação de diretrizes, é entendida a utilização de smart contracts em Padma, A.; Ramaiah, M. (2024), de um Broker IoT que utiliza recriptografia por proxy para gerir os acessos (RIVADENEIRA et al., 2024), um controle de acesso a dados descentralizado e auto-gerenciado (SAIDI et al., 2022) e um sistema que utiliza criptografia baseada em atributos (TOMAZ et al., 2020).

Passando para o terceiro eixo, anonimização ou pseudoanonimização, percebeu-se a utilização de hashes em credenciais (ABBAS et al., 2022) e hashes em chaves públicas (LV et al., 2019), privacidade diferencial local (KHALIQ et al., 2022), um esquema de autenticação anônima denominado zero-knowledge succinct noninteractive argument of knowledge (LUONG, D. A.; PARK, J. H., 2022), um método criptográfico conhecido por zero-knowledge proof (SAIDI et al., 2022) e armazenamento das informações de identidade dos usuários em compartimento dedicado (XIE et al., 2019). No que tange os estudos de Zou et al. (2020) e Sutradhar et al. (2024), não foram especificados os detalhes pertinentes ao respectivo eixo.

Tabela 3. Identificação dos eixos presentes nos estudos analisados

Autor	Área de aplicação	Descrição	i.	ii.	iii.
KHALIQ, A. A. et al., 2022	Smart Parking	Desenvolve um sistema de recomendação de estacionamento utilizando criptografia de curva elíptica e privacidade diferencial local para proteger os dados dos usuários		x	x
LV, P. et al., 2019	IoT	Propõe um modelo de publicação/assinatura orientado à IoT que preserva a privacidade usando blockchain e criptografia de chave pública		x	
PADMA, A.; RAMAIAH, M., 2024	Smart Cities	Apresenta um framework para cidades inteligentes usando blockchain e contratos inteligentes para gerenciar a privacidade dos dados urbanos		x	
ABBAS, S. et al., 2022	IoUT	Aplica blockchain para autenticação preservando a privacidade e detecção de nós maliciosos em redes IoUT		x	
STODT, F. et al., 2024	IIoT	Propõe uma arquitetura de auditoria de chão de fábrica preservando a privacidade usando blockchain		x	
XIE, L. et al., 2019	VANETs	Explora a segurança e confiança na IoT em redes 5G-VANETs habilitadas por SDN utilizando blockchain		x	
MANTEY, E. A. et al., 2023	IoMT	Desenvolve uma técnica habilitada por blockchain para sistemas de recomendação médica que preservam a privacidade usando aprendizado federado	x	x	
JIN, H. et al., 2021	IoMT	Combina aprendizado federado e blockchain para a Internet das Coisas Médicas (IoMT), garantindo a privacidade dos dados médicos	x	x	
ZOU, S. et al., 2020.	MCS	Desenvolve um sistema de crowdsensing móvel preservando a privacidade baseado em blockchain, focado na privacidade de localização		x	x
SAIDI, H. et al., 2022	IoMT	Apresenta um modelo de autogestão descentralizada do controle de acesso a dados de saúde baseado em blockchain	x	x	
MA, Z.; ZHANG, J., 2023	IoD	Propõe um controle de acesso a dados eficiente e consciente da privacidade em sistemas IoD baseados em blockchain	x	x	
SHE, W. et al., 2019	Smart Homes	Propõe um blockchain de consórcio homomórfico para preservar a privacidade dos dados sensíveis em sistemas de smart home		x	x
TOMAZ, A. E. B. et al., 2020	IoMT	Aplica provas de conhecimento zero não interativas (NIZK) e blockchain para preservar a privacidade em sistemas de saúde móvel		x	x

Autor	Área de aplicação	Descrição	i.	ii.	iii.
MA, M.; SHI, G.; LI, F., 2019	IoT	Propõe uma arquitetura de gerenciamento de chaves distribuída orientada para a privacidade baseada em blockchain		x	
LUONG, D. A.; PARK, J. H., 2022.	IoMT	Desenvolve um sistema de saúde baseado em IoT que preserva a privacidade utilizando zk-SNARK e blockchain		x	x
QASHLAN, A. et al., 2021.	Smart Homes	Explora mecanismos de preservação da privacidade em smart homes utilizando blockchain		x	
RIVADENEIRA, J. E. et al., 2024	HiTLCPS	Propõe um modelo unificado de preservação da privacidade com IA na periferia para sistemas ciber-físicos com humanos no loop		x	
SUTRADHAR, S. et al., 2024	IoMT	Apresenta uma abordagem baseada em blockchain para melhorar o gerenciamento de identidade e acesso utilizando Hyperledger Fabric e OAuth 2.0	x	x	

Legenda: i. Controle sobre os dados; ii. Implementação de diretrizes; iii. Anonimização ou pseudoanonimização
Fonte: Os autores.

Considerações Finais

A presente RSL analisou trabalhos desenvolvidos no âmbito das PETs, em um contexto de dispositivos IoT que se utilizam de tecnologia blockchain. A partir dos dados coletados, foi possível notar preocupações como a presença de um controle de acesso nos dados trafegados, mecanismos que facilitem a escolha de quais desses dados serão compartilhados com empresas e outras entidades, e a anonimização ou pseudoanonimização da identidade dos usuários. Apesar de essas três dimensões não estarem presentes em todos os estudos, é visível que as questões envolvendo privacidade e seu controle são discutidas e implementadas em ecossistemas IoT.

Em trabalhos futuros, sugere-se a classificação de projetos IoT que utilizem tecnologia blockchain considerando também os eixos internos do desenho proposto por Cha et al. (2019), sendo eles a Proteção de Dados Pessoais, a Autorização Anônima, a Divulgação Parcial de Dados e a Preservação Holística da Privacidade.

Referências

ABBAS, S. et al. Blockchain Based Privacy Preserving Authentication and Malicious Node Detection in Internet of Underwater Things (IoUT) Networks. **IEEE Access**, Piscataway, v. 10, 25 out. 2022, p. 113945–113955. Disponível em: <https://ieeexplore.ieee.org/document/9928190>. Acesso em: 15 abr. 2024.

BRERETON, P. et al. Lessons from applying the systematic literature review process within the software engineering domain. **Journal of Systems and Software**, Amsterdã, v. 80, n. 4, abr. 2007, p. 571–583. Disponível em: <https://www.sciencedirect.com/science/article/pii/S016412120600197X>. Acesso em: 15 abr. 2024.

CAVOUKIAN, A. **Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices**. Ontario, 2009. Disponível em: <https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf>. Acesso em: 15 abr. 2024.

CHA, S. C. et al. Privacy enhancing technologies in the internet of things: Perspectives and challenges. **IEEE Internet of Things Journal**, Nova York, v. 6, n. 2, 1 abr. 2019, p. 2159–2187. Disponível em: <https://ieeexplore.ieee.org/document/8515008>. Acesso em: 15 abr. 2024.

CROSBY, M. et al. BlockChain Technology: Beyond Bitcoin. **Applied Innovation Review**, Berkeley, n. 2, jun. 2016. Disponível em: <https://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf>. Acesso em: 15 abr. 2024.

DERMEVAL, D.; COELHO, J. A. P. de M.; BITTENCOURT, I. I. **Mapeamento Sistemático e Revisão Sistemática da Literatura em Informática na Educação**. In: JAQUES, P. A.; SIQUEIRA; S.; BITTENCOURT, I.; PIMENTEL, M.. (Org.) Metodologia de Pesquisa Científica em Informática na Educação: Abordagem Quantitativa. Porto Alegre: SBC, 2020. (Série Metodologia de Pesquisa em Informática na Educação, v. 2) Disponível em: <https://metodologia.ceie-br.org/livro-2>. Acesso em: 15 abr. 2024.

JIN, H. et al. Cross-Cluster Federated Learning and Blockchain for Internet of Medical Things. **IEEE Internet of Things Journal**, Nova York, v. 8, n. 21, 1 nov. 2021, p. 15776–15784. Disponível em: <https://ieeexplore.ieee.org/document/9434416>. Acesso em: 15 abr. 2024.

KHALIQ, A. A. et al. A Secure and Privacy Preserved Parking Recommender System Using Elliptic Curve Cryptography and Local Differential Privacy. **IEEE Access**, Piscataway, v. 10, 1 jun. 2022, p. 56410–56426. Disponível em: <https://ieeexplore.ieee.org/document/9775988>. Acesso em: 15 abr. 2024.

KITCHENHAM, B. et al. **Guidelines for performing Systematic Literature Reviews in Software Engineering**. Versão 2.3. Durham, 9 jul. 2007. Disponível em: <https://legacyfileshare.elsevier.com/promis_misc/525444systematicreviewsguide.pdf>. Acesso em: 15 abr. 2024.

LUONG, D. A.; PARK, J. H. Privacy-Preserving Blockchain-Based Healthcare System for IoT Devices Using zk-SNARK. **IEEE Access**, Piscataway, v. 10, 23 mai. 2022, p. 55739–55752. Disponível em: <https://ieeexplore.ieee.org/document/9780211>. Acesso em: 15 abr. 2024.

LV, P. et al. An IOT-oriented privacy-preserving publish/subscribe model over blockchains. **IEEE Access**, Piscataway, v. 7, 23 mar. 2019, p. 41309–41314. Disponível em: <https://ieeexplore.ieee.org/document/8674745>. Acesso em: 15 abr. 2024.

MA, M.; SHI, G.; LI, F. Privacy-Oriented Blockchain-Based Distributed Key Management Architecture for Hierarchical Access Control in the IoT Scenario. **IEEE Access**, Piscataway, v. 7, 10 mar. 2019, p. 34045–34059. Disponível em: <https://ieeexplore.ieee.org/document/8664491>. Acesso em: 15 abr. 2024.

MA, Z.; ZHANG, J. Efficient, Traceable and Privacy-Aware Data Access Control in Distributed Cloud-Based IoD Systems. **IEEE Access**, Piscataway, v. 11, 2 mai. 2023, p. 45206–45221. Disponível em: <https://ieeexplore.ieee.org/document/10114388>. Acesso em: 15 abr. 2024.

MANTEY, E. A. et al. Blockchain-Enabled Technique for Privacy-Preserved Medical Recommender System. **IEEE Access**, Piscataway, v. 11, 26 abr. 2023, p. 40944–40953. Disponível em: <https://ieeexplore.ieee.org/document/10109503>. Acesso em: 15 abr. 2024.

PADMA, A.; RAMAIAH, M. Blockchain Based an Efficient and Secure Privacy Preserved Framework for Smart Cities. **IEEE Access**, Piscataway, v. 12, 7 fev. 2024, p. 21985–22002. Disponível em: <https://ieeexplore.ieee.org/document/10426751>. Acesso em: 15 abr. 2024.

PAPPACHAN, P. et al. Towards Privacy-Aware Smart Buildings: Capturing, Communicating, and Enforcing Privacy Policies and Preferences. In: 2017 IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW), 37., 2017, Atlanta. **Anais…** Atlanta: IEEE Xplore, 2017. Disponível em: <https://ieeexplore.ieee.org/document/7979816>. Acesso em: 15 abr. 2024.

PETERS, M. D. J et al. **The Joanna Briggs Institute reviewers' manual 2015: methodology for JBI scoping reviews**. Adelaide: The Joanna Briggs Institute. Disponível em: <http://joannabriggs.org/assets/docs/sumari/Reviewers-Manual_Methodology-for-JBI-Scoping-Reviews_2015_v2.pdf>. Acesso em: 15 abr. 2024.

QASHLAN, A. et al. Privacy-Preserving Mechanism in Smart Home Using Blockchain. **IEEE Access**, Piscataway, v. 9, 20 jul. 2021, p. 103651–103669. Disponível em: <https://ieeexplore.ieee.org/document/9492086>. Acesso em: 15 abr. 2024.

RIVADENEIRA, J. E. et al. A unified privacy preserving model with AI at the edge for Human-in-the-Loop Cyber-Physical Systems. **Internet of Things**, Amsterdã, v. 25, 1 abr. 2024. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2542660523003578>. Acesso em: 15 abr. 2024.

SAIDI, H. et al. DSMAC: Privacy-Aware Decentralized Self-Management of Data Access Control Based on Blockchain for Health Data. **IEEE Access**, Piscataway, v. 10, 19 set. 2022, p. 101011–101028. Disponível em: <https://ieeexplore.ieee.org/document/9895264> . Acesso em: 15 abr. 2024.

SHE, W. et al. Homomorphic Consortium Blockchain for Smart Home System Sensitive Data Privacy Preserving. **IEEE Access**, Piscataway, v. 7, 15 mai. 2019, p. 62058–62070. Disponível em: <https://ieeexplore.ieee.org/abstract/document/8715767>. Acesso em: 15 abr. 2024.

STODT, F. et al. Blockchain-Based Privacy-Preserving Shop Floor Auditing Architecture. **IEEE Access**, Piscataway, v. 12, 14 fev. 2024, p. 26747–26758. Disponível em: <https://ieeexplore.ieee.org/document/10436670>. Acesso em: 15 abr. 2024.

SUTRADHAR, S. et al. Enhancing identity and access management using Hyperledger Fabric and OAuth 2.0: A blockchain-based approach for security and scalability for healthcare industry. **Internet of Things and Cyber-Physical Systems**, Beijing, v. 4, p. 49–67, 1 jan. 2024. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2667345223000470>. Acesso em: 15 abr. 2024.

TOMAZ, A. E. B. et al. Preserving privacy in mobile health systems using non-interactive zero-knowledge proof and blockchain. **IEEE Access**, Piscataway, v. 8, 9 nov. 2020, p. 204441–204458. Disponível em: <https://ieeexplore.ieee.org/document/9252935>. Acesso em: 15 abr. 2024.

XIE, L. et al. Blockchain-based secure and trustworthy internet of things in SDN-enabled 5G-VANETs. **IEEE Access**, Piscataway, v. 7, 29 abr. 2019, p. 56656–56666. Disponível em: <https://ieeexplore.ieee.org/document/8701642>. Acesso em: 15 abr. 2024.

ZOU, S. et al. CrowdBLPS: A Blockchain-Based Location-Privacy-Preserving Mobile Crowdsensing System. **IEEE Transactions on Industrial Informatics**, Piscataway, v. 16, n. 6, 1 jun. 2020, p. 4206–4218. Disponível em: <https://ieeexplore.ieee.org/document/8926541>. Acesso em: 15 abr. 2024.